Intro:

Hello and welcome to the CPA Australia podcast, your weekly source for accounting, education, career and leadership discussion.

Michael Jeremenko:

Hi everyone. Thank you for joining us and welcome to CPA Australia's podcast on cyber security in the COVID-19 world. Today is the 2nd of July, 2020 and this is one of the first podcasts hosted by the ACT division of CPA Australia. My name's Michael Jeremenko and as a member of CPAs, public sector and management accountants committee in ACT, I'm proud to be hosting today's podcast on cyber security and with a very special guest who I'll introduce shortly. I'm sure our listeners are interested in this topic, cyber security, what is it, why is it important and what does it mean during COVID-19? We're becoming more and more reliant on technology, everyone uses mobile phones and computers for just about everything we do. Our lives are controlled by technology. What happens when our technology, our personal and secure data becomes compromised? How can we protect ourselves from these outside and unknown threats? What impact is COVID having on our data and our security?

These are some of the questions we'll cover off in today's podcast. So I'm glad to be welcoming a very special guest today, Gai Brodtmann. Gai is a board member of Old Parliament House in Canberra, a member of the Australian Strategic Policy Institute Council and Sapien Cyber Advisory Board, the presenter and panellist at the National Security College and Australian Defence College and contributor to The Strategist. Gai served as a member for Canberra from 2010 – 2019, she was a shadow assistant minister for cybersecurity & defense from 2016 – 2019. And shadow parliamentary secretary for defense from 2013 – 2016. Before her political career, Gai ran her own small business for 10 years and worked for the Federal Government, mostly within the Department of Foreign Affairs and Trade and Attorney Generals. Gai's national security policy interests include cyber security across a broad range spheres women, peace and security, critical infrastructure, capability sustainment, and sovereign capacity. Welcome Gai Brodtmann and thank you for joining us today.

Gai Brodtmann:

Thank you, Michael. And thank you very much for the CPA for putting on this podcast.

Michael Jeremenko:

Well, you've had a very diverse career, ranging from running a small business, working in the public service, serving as a member of parliament, consulting to the Defence Department and now working in national security. So Gai, what led to your interest in national security and in particular, why cyber security?

Gai Brodtmann:

Well, my interest in national security and international relations really began when I was a student at the Australian National University where I studied Middle Eastern politics and it was during the time that the Russians had invaded Afghanistan. So that was where my interest really began. Then I worked in the Department of Foreign Affairs and Trade for a number of years, and I had a posting to India and worked on the Middle East desk and was involved in the normalisation of the relationship with Iran, which was a huge career highlight for me. After that, I consulted in Defence for nearly a decade before I went into politics and that's where my interest was really honed, particularly on capability, acquisition and

sustainment because sustaining a piece of kit cost 10 times more than it actually does to buy it and so I was interested in how we could get greater efficiencies in that system.

My interests continued into politics when I was, as you've mentioned, on the Public Accounts and Audit Committee and the Foreign Affairs and Defence and Trade Committee, when I had the shadow responsibility for cyber security and I actually requested that portfolio. In terms of my cyber security interests, I became really interested in it around early 2010, around that period when there were a lot of stories about sexting. I don't know whether any of your listeners will remember that, but there were a number of schools in Sydney where there was this sexting going on, where young people were sending these lurid messages and images that really put them in a compromising position and it was causing a great deal of concern, naturally to their parents and their school community. And I was interested at that stage about what that actually meant in terms of privacy settings and privacy policy, privacy public policy. Because I just wondered if things were changing, particularly amongst younger people in terms of their perceptions of privacy and whether we needed to respond as public policy makers.

Then it diversified into critical infrastructure and protecting our critical infrastructure and standards and the vulnerability posed by our supply chains and international norms and cyber security of government agencies, because audits have found that a large number, too many, do not comply with mandated standards. Also, I became interested in how do we address the skills gap, we're currently about 17,000 experts down and how do we train them for the future and how do we ensure that they're accredited and fit for purpose. Also interested in how we accredit courses and the training for these experts, and even down to the dial the geek that you ring up to come and fix your computer, whether that person is actually accredited and has actually undergone any training and is someone you can trust.

Also interested in getting more women into cyber security, we're currently, depending on the figures, we are a lot better than we were. It was around 11%, a number of years ago, we're about 25% now, but we can still do with more. And also the main driver for me on cyber security is the fact that I want to ensure that the innovation and technology of the future, realises and unleashes potential, that it liberates our community and it doesn't enslave it.

Michael Jeremenko:

That's fantastic. And just with COVID, COVID's changed how we work and how we live, in particular, all of us are working from home. We're reading all these recent articles around the place, more recently from Scott Morrison, where there's warnings, Australia's coming under this escalating series of cyberattacks from sophisticated hackers and the government is putting a lot of money into cyber security. You're talking somewhere around the magnitude of $1 billion. What's your view on these escalating cyber security threats since, I guess, the COVID-19 pandemic started back around February and March?

Gai Brodtmann:

Well, there's been a number of scams and phishing exercises that have been linked to supposed information campaigns on COVID-19. And I've got to say the Australian Cyber Security Centre has done a terrific job, in my view, of bringing this to community attention. They're the kinds of emails that people are receiving and links and apps and texts that look like they're official communications and they're not. So there has been an increase in the number of COVID-19 specific phishing attempts, that basically look helpful when they are not helpful at all. There's also the risks, the increased risk that has been posed and the increased challenge that's been posed from people from working from home, with the

accompanying distractions like children doing homeschooling, partners also working from home and interruptions that just come from the reality of being in the home environment when you're working.

There's also been, and I think that this has been helpful in many ways, people have really started to think about their own cybersecurity at home, in terms of the increased vulnerability of their data and how they manage securing that environment. So this period of COVID, as a result of the scamming exercises and as a result of people working from home, has exposed people to a greater vulnerability in many ways, and exposed them to the fact that they are exposed. And again, it's highlighted the fact that everyone, cybersecurity is everyone's responsibility and that people need to become cyber aware, they need to stay smart online and they need to have the tools to do that.

Michael Jeremenko:

It's coming across more and more that employers are warning employees to watch out for these sorts of phishing emails and the like, and I guess there must be some sort of investment going on in the background. What are the technologies that you're aware of, due to COVID-19, that could strengthen cyber security, something that businesses can take on board or employers?

Gai Brodtmann:

Well, new technologies are arising every day, but there's been a lot of clever solutions that have been around for a while, particularly in the area of portable and affordable cybersecurity devices that don't require an ICT department to support you. Because I think that this is the issue that we're facing at the moment for many Australians, is the fact that they used to having the security of being in an office environment and having all the support, the ICT support systems behind them in that office environment. Now they're at home and they are feeling exposed, which is why they need to be empowered to actually manage their cyber security settings at home. As I said, before COVID, the focus was very much on securing, for many Australia's, securing the office environment. Now that people are working from home, they're focusing more on how to secure the home and most importantly, how to secure that interaction between the home and the office.

Now, I don't want to mention any names, but there are number of innovative Australian-made solutions allowing people to work on secure documents remotely, or secure through their router. The challenge in my view is for Australians to actually, and particularly large agencies and large organisations and government agencies, to actually look at those innovative solutions, to focus, the big names that are out there, to focus on those innovative solutions that are around, those Australian-made solutions around, everyone's talking a good game on sovereign capability at the moment, but we actually need to follow through that in cybersecurity. We've got a number of world-class Australian-made solutions here, now government agencies and large companies need to actually put their money where their mouth is.

Michael Jeremenko:

Fantastic. So basically, generally governments are risk averse and what you're saying is that there's some cost-effective solutions out there, maybe easy solutions to implement, that can be implemented. But I think what you're saying is organisations need to think broader and maybe not be as risk averse in some of those areas.

Gai Brodtmann:

Yeah. And this is an issue that I pursued when I was in parliament, is the fact that these small outfit, or these innovative outfits, these Australian-made outfits, all they're asking is for a government agency or a

large organisation just to buy one, just to try it out. And that's all they're asking, they don't have to commit to, in the first instance, they don't actually have to commit to a huge contract, but if they can just buy one and see how innovative this technology is, how innovative their solutions are, then it would open their eyes to a range of possibilities. There is a risk aversion in government agencies and as someone who was on the Public Accounts and Audit Committee, someone formerly deputy chair of that committee, I do understand, this is hard earned Australian taxpayers money, and people do need to be careful about the way it's managed and they do need to be transparent in the way it's managed.

But there is a big push, that's been one of the key messages that's come out of COVID, is this need to explore, to better develop as sovereign capability, that sovereign capability in cyber security exists and we just need large organisations and government agencies to actually take a punt and actually put their money where their mouth is.

Michael Jeremenko:

Gai, so working from home, how can we better manage the cyber security risk, especially using our own computers, file sharing accounts and our own internet connections, et cetera?

Gai Brodtmann:

So this rule doesn't actually apply just for working from home, it needs to apply every day. I mean, I'm hoping that the lockdown and working from home has reminded people about the importance of cyber hygiene and that we actually see a cultural shift in all Australians as a result of the lockdown, because we've got to start seeing this as a risk, and we've got to start developing controls to minimise those risks. Cyber security is all about risk management, and we need to start seeing it that way. We need to treat our cyber security in the same way that we treat our physical security. When we leave home, we lock the door. When we leave our car, we lock the car door. We set the alarm if we have an alarm system, we have a number of controls in place to mitigate the risks to our physical environment.

Why don't we have the same controls in place, why don't we have the same controls in place to mitigate the risks in the cyber security environment? Because think about what's actually on our computer, most businesses have all their business data on their computer. The whole business, the success of their business relies on their computer and so they need to actually treat that as a very, very precious source of data and they need to develop the strategies and the controls to actually manage the risks that could potentially compromise or attack that data.

In terms of people's computers, people don't cover up the camera on their computer, that potentially opens them to being seen. They don't regularly update and I'll come to that in a minute. We don't shut it down at night, our computer, our desktop computer at home. Again, it just minimises risks, yeah, it does minimise risks. In terms of our devices, our portable devices, our mobile devices, people take their mobile or their iPad into their bedroom. Some people take their mobile or their iPad into the bathroom, or the toilet. Think about what could actually, if the camera's going, if those right security settings aren't going, then what is potentially, they're being watched.

So a number of key principles apply here, and these are principles that are universal. First up, you've got to have a strong password. Now there's mixed views on the complexity of the password. There's some people who think you've got to have lots of symbols and it's got to be really long and you've got to have lots of numbers. There's, as I said, mixed views on that, the main aim is to have a strong password. Now I'm not sure whether people, your members would be aware of this, but the most commonly used passwords in data breaches are pretty obvious. And the fact that people are still using these passwords in this day and age, in the multi-millions, is breathtaking. I'm talking here one, two,

three, four, five, six. QWERTY. I love you. One, one, one, one, one. These are commonly used passwords and quite often people use them across all their documents, that have basically been found to be easily penetrable and the cause of data breaches.

So I've got my own cyber security people, I'm a micro-business, but I've got my own cybersecurity people who've helped me set up, to secure as far as possible, my desktop environment, my work environment, and they have put me on to two sites and so I do recommend that people actually have a look at these sites. One is, how secure is my password, you type in your password and that actually checks the security of your password. And there's another terrific one too, that I've used as well, which is a password generator, it's called last pass password generator. So that actually generates a password for you that is really, really secure. So I can't underscore the point enough that you've got to start with having strong passwords and 'I love you' or 'fluffy' one or the name of your partner and one, two, three, is not a strong password.

Secondly, you've got to backup. You've got to backup your data, daily ideally, if not regularly. It means that if you're a victim of an attack, you've got the last lot of saved data, it can be retrieved. You need to install updates when they pop up. Now, I know that everyone finds this a pain, but it is vitally important to make sure that you've got the latest software on your system. Don't press the remind me later button and then basically forget it. Particularly if you're working from home, one of the really important thing is, so that you're not distracted by it, to minimise the distractions and the tiredness, is to actually have a break. So I recommend that if you do see the update popup, then use the time to go and have a cup of coffee, have a glass of water, have a cup of tea, go and stand outside and just breathe in the beautiful fresh air and actually install those updates. Again, vital important, do not press the remind me later button.

There's another piece of advice that has been provided too, is shutting down your computer every night or regularly, and this applies to devices too. It helps it reset so that if bad software has got in, then basically it's going to make it, you've reset everything and so it's been refreshed. And also use VPN so it's harder to be targeted or seen by outsiders. Only download apps from reputable developers. And that usually doesn't mean using free trials or free anything, only use reputable apps and programmes, don't use free trials or free anything. Explore the security settings on your Fitbit and your mobile devices because essentially they're tracking devices. I mean, I don't know whether many of your listeners saw, a few years ago, there was a story about secret US bases were being identified in space through Fitbit's that were being worn by soldiers running around the perimeter of the base.

And so again, it was a tracking device that could actually see the outline of these bases. I've heard stories and many of your listeners probably would have heard these too, where mobile devices and televisions and dolls have been used to spy on women fleeing domestic violence. So I do encourage all your members to take the security setting seriously and actually try and make your devices, your Fitbit or your mobile or your iPad or your desktop, try and make them as secure as possible.

Michael Jeremenko:

Thank you Gai, fantastic tips, principles, and habits that we need to look at implementing. I know myself, I've been always at times perhaps thinking of putting an easier password in, rather than a more difficult one, due to time constraints, but we definitely need to, I think, take the time aside and think about all those tips and principles that you just mentioned. So Gai, in terms of CPAs and accountants, what can we do to reduce any of these cyber security threats?

Gai Brodtmann:

First up, CPAs and accountants need to treat cyber security, the risk of cyber security in the same way they treat financial risks. This is a risk management exercise and accountants are very au fait with risks and they're very au fait with controls and strategies to mitigate risks and manage risks, they need to treat cyber security in the same way they treat our financial risks. Because think about it, if you have been, if you are the victim of a cybercriminal or the victim of an attack, that could potentially see your business go under. Now, I know that there's a broad range of people, CPAs, who are listening today in terms of CPAs from government agencies, CPAs from small business, CPAs with their own businesses, so I do encourage them all, no matter what size your organisation, no matter what type your organisation, to treat this the same as a financial risk, the same as any other risk and set up the strategies, the controls to mitigate and manage that risk.

Secondly, you need to be aware that you're holding incredibly sensitive data and how would you feel if it was leaked and how would you feel if you found out it was being sold on the dark web. Now, a friend of mine used to work at Telstra and she developed the five knows and I'm talking here, the K-N-O-W-S, knows, and I think they're applicable to every organisation, particularly your members and they're available on the web. First up, know the value of your data, know who has access to your data, know where your data is, know how well your data is protected and know who is protecting your data.

CPAs, accountants should also have data management protocols in place, so you know exactly who's got access to what data and importantly, it makes you think about who actually needs the access to what data. It makes you take a long, hard look at that so that you don't have data, very highly sensitive, incredibly sensitive data available and accessible to everyone. And also CPAs and your accounts, your members, need to also ask, "Have we got a data breach strategy in place? What would we do if we were breached? Who do we need to notify for a breach?" Because there are regulations around all this now. So it's having a data management protocol in place, but also a strategy, should you be breached, unfortunately, should you be breached, how are you going to actually manage that and ensure that you can get your business back to business as soon as possible.

And also in terms of those who've got clients, I mean, how are you going to notify your clients? That's going to be a very tough conversation. So these CPAs, your members, need to be having these conversations and need to be setting up these protocols. Also, they need to be thinking about supply chains and the suppliers that they work with. I mean, do they have cyber secure environments? Because if you send an email in and it's contaminated, then it could basically launch malware into your business environment. So that's why that you also need to think about your suppliers as well. Now I've been pushing for some sort of accreditation of suppliers and others in the past, in terms of a certification process. I mean, this would need to be done in consultation with the small business associations particularly, but how do we actually ensure businesses that their suppliers are cyber secure and that they're not going to potentially launch malware into their systems, because there's been many instances of that. How can we get some sort of certification that we can trust that particular supplier?

Most importantly, CPAs and your members need to go back to the question about cyber hygiene in your organisation and that human factor, because cyber security is as much, if not more, about the human element than it is about the technical element. So are your people in your organisation cyber savvy? Have they been trained on cyber security? Has their training been updated? Does your organisation have a cyber hygiene culture? Because insider threats are alive and real, and I'm not talking here about those with a malicious intent, although they do exist, there's those who basically unwittingly launch, through a phishing exercise or through a scam, launch malware into a business environment. So by having your people aware of what they need to look for, what they need to be concerned about, what they need to be alert to, allows you to have some level of assurance that you do actually have a cyber savvy workforce.

I mean, last year, a Verizon study found that 94% of malware was delivered by email. If people aren't aware of what to look for, if they add alert to the risks of the environment, then they could potentially launch that malware by clicking a link in the email. Also, have you had a cyber security assessment done in your organisation? There's plenty of organisations around there, again, I'm not talking the big four and I'm not talking major companies here, there's plenty of small and medium outfits that are out there, that are reasonably priced, that can help cyber secure micro and small and medium organisations. As I mentioned before, I've used one myself.

So in my view, if you haven't already, then please go out and get an assessment done of your environment. And you don't have to pay the earth for it, there's some very competitively priced, small and medium outfits that can do it for you. And finally, if you're a government agency, I've mentioned those statistics beforehand, it's a great concern about the fact that so few of our government agencies, through audits by the National Audit Office have actually been found to be cyber resilient. So I'd ask the question, to your … if you're in a government agency, does your organisation comply with mandated cyber security standards?

Michael Jeremenko:

Fantastic. Cybercrime insurance, is this something new and is this something maybe businesses should consider? Is it worth taking up? What's your view on that?

Gai Brodtmann:

Well, nothing can replace proper cyber hygiene and a strong cyber culture in an organisation and appropriate protocols and appropriate training and appropriate awareness and education. So that should be the number one priority of any organisation, be it micro, small, medium, or large. But if you are considering cyber insurance, you need to do it against, again, this gets back to this issue of being, it's a risk issue, it's a risk management issue. So in terms of consideration of cyber insurance, it needs to be done against your risk appetite and your risk tolerance. You need to ask the question, can you afford the risk of not actually having cyber insurance and also what can you afford? Because it isn't cheap, but it is just in my view, just another cost of doing business, for some outfits, it's like professional indemnity, it's like public liability insurance, it is just another cost of doing business.

So you need to actually look at first up, identify the fact that cyber security is a risk, secondly, assess a cyber risk in terms of your risk appetite and your risk tolerance, and then work out what would happen if you were a victim of, consider, do some scenario planning on what would happen if you were a victim of a cyber attack or a cyber incident, and then assess it against that. You also need to look at policies quite closely because there's a number of elements, like any insurance policy that you can have, there's a number of optional extras, so you need to think about what you actually want in your policy. Would you want to just cover data breaches? Would you want to cover extortion threats? Would you want to cover replacement of technology? Would you want to cover public relations, should a data breach occur and you needed to get information out to your clients? So these are all factors that need to be considered, but most importantly, you need to consider cyber security as a risk issue and cyber insurance needs to be considered in the context of your organization's risk management strategy.

Michael Jeremenko:

Thank you Gai. It's been a fantastic podcast. Is there anything you'd like to add to our listeners today before we wrap up?

Gai Brodtmann:

Thanks, Michael. The main message is don't be frightened by the cyber security environment. You feel empowered in managing the risks to your home security, to your car security, you just need to treat the risks in the cyber security environment as the same. Follow those key principles, they will really help you manage and mitigate those risks because most importantly, the future in technology offers so much potential and I want all Australians to realise that potential and they need to feel empowered and in control to be able to do that. So follow those key principles, don't be frightened, treat it as a risk and manage it in the same way you manage the risk to your home and your car security. And finally, so to get more tips on what to do visit www.cyber.gov.au, it's got some terrific information for micro businesses, for small businesses, for large organisations, for critical infrastructure, government agencies and individuals. And it also keeps you up to date with what's actually happening in terms of scams and phishing exercises and areas of activity for cyber criminals. Most importantly, it keeps you up to date on how to stay smart online.

Michael Jeremenko:

Well Gai, personally, I've found your conversation on cyber security in the COVID world interesting and insightful. I do thank you for sharing your contemporary views, principles and tips, and some of the better cultural habits we all need to think about. Also, you mentioned need to implement strategies and security assessments and to think outside the square and to be more creative. It's definitely made us all more aware about an extremely important subject, which will no doubt be with us for some time. Technology and computers, we're so reliant on it, it governs our daily lives. Technology's becoming smarter and those using it are also becoming smarter and those who want to obtain our data for wrongful purposes, are getting smarter at looking at obtaining it. On behalf of CPA Australia and our listeners, we thank you so much for your time in joining us today. Thank you Gai Brodtmann.

Gai Brodtmann:

Thank you Michael.

Michael Jeremenko:

This concludes our podcast today, and thank you to all our listeners for joining us.

Outro:

Thanks for listening to the CPA Australia podcast. For more information on today's episode, please visit the show notes at www.cpaaustralia.com.au/podcast. Never miss an episode by subscribing to our podcast on Apple podcasts, Spotify, or Stitcher.